VIII kadencja

KANCELARIA SEJMU
Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 7)**

z dnia 27 stycznia 2016 r.

Pełny zapis przebiegu posiedzenia

Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii (nr 7)

27 stycznia 2016 r.

Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii, obradująca pod przewodnictwem posła **Pawła Pudłowskiego (N)**, przewodniczącego Komisji, rozpatrzyła:

– wniosek prezydium Komisji w sprawie powołania stałego doradcy Komisji – kontynuacja;

– informację o projekcie dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (tzw. Dyrektywa NIS).

W posiedzeniu udział wzięli: **Witold Kołodziejski** sekretarz stanu w Ministerstwie Cyfryzacji wraz ze współpracownikami, płk **Jacek Gawryszewski** zastępca szefa Agencji Bezpieczeństwa Wewnętrznego wraz ze współpracownikami, **Marek Kubiak** dyrektor Rządowego Centrum Bezpieczeństwa wraz ze współpracownikami, **Jacek Matyszczak** dyrektor Departamentu Bezpieczeństwa Telekomunikacyjnego Urzędu Komunikacji Elektronicznej, kom. **Marcin Kuskowski** pełnomocnik Komendanta Głównego Policji do spraw bezpieczeństwa cyberprzestrzeni wraz ze współpracownikami oraz **Marcin Kanarski** ekspert Polskiej Izby Informatyki i Telekomunikacji.

W posiedzeniu udział wzięły pracownice Kancelarii Sejmu: **Ewa Gast** i **Julia Popławska** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodniczący poseł Paweł Pudłowski (N):

Dzień dobry. Witam państwa bardzo serdecznie. Otwieram posiedzenie Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Witam panie i panów posłów oraz zaproszonych gości.

Stwierdzam kworum.

Porządek dzisiejszego posiedzenia obejmuje, po pierwsze, rozpatrzenie wniosku prezydium Komisji w sprawie powołania stałego doradcy Komisji – jest to kontynuacja z poprzedniego posiedzenia – po drugie, rozpatrzenie informacji o projekcie dyrektywy Parlamentu Europejskiego i Rady w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii (tzw. Dyrektywa NIS). Powyższy porządek oraz materiały członkowie Komisji otrzymali. Czy są uwagi do porządku dziennego? Jeżeli nie ma, stwierdzam, że Komisja przyjęła porządek dzienny posiedzenia bez zmian.

Przystępujemy do realizacji pierwszego punktu porządku dziennego. Na posiedzeniu w dniu 14 stycznia Komisja przystąpiła do rozpatrywania wniosku prezydium Komisji w sprawie powołania stałego doradcy. W głosowaniu zdecydowano o odroczeniu wyboru do kolejnego posiedzenia, tzn. dzisiejszego, w dniu 27 stycznia. Chciałbym państwa poinformować, że w dniu dzisiejszym wpłynęło pismo następującej treści – pozwolę sobie odczytać pismo skierowane na ręce przewodniczącego Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu Rzeczypospolitej Polskiej:

„Szanowny Panie Przewodniczący, informuję, iż rezygnuję z ubiegania się o powołanie na stanowisko stałego doradcy Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Jednocześnie chciałbym serdecznie podziękować za możliwość przedstawienia swojej kandydatury.

Z poważaniem,

dyrektor Naukowej i Akademickiej Sieci Komputerowej

Michał Chrzanowski”.

Wobec rezygnacji pana dyrektora nie będziemy kontynuowali rozmowy na ten temat.

Wobec tego przechodzimy do realizacji drugiego punktu porządku dziennego. Proszę pana dyrektora Macieja Gronia o przedstawienie dyrektywy NIS. Chciałbym tylko państwu powiedzieć, że dostaliśmy pismo wprowadzające od pani minister, która przeprasza, że nie ma jej osobiście i upoważnia pana dyrektora do przedstawienia wymienionej dyrektywy. Bardzo proszę, panie dyrektorze.

Dyrektor Departamentu Społeczeństwa Informacyjnego Ministerstwa Cyfryzacji Maciej Groń:

Dziękuję uprzejmie. Nazywam się Maciej Groń. Jestem dyrektorem Departamentu Społeczeństwa Informacyjnego w Ministerstwie Cyfryzacji.

Chciałbym przedstawić krótką informację na temat prac, które są prowadzone przy dyrektywie NIS. Proszę państwa, przede wszystkim chciałbym powiedzieć, że cały czas mówimy o projekcie dyrektywy. Dyrektywa nie jest jeszcze przyjęta. Mamy nadzieję, że będzie przyjęta bardzo szybko. Proszę państwa, sam projekt dyrektywy w sprawie środków mających na celu zapewnienie wspólnego wysokiego poziomu bezpieczeństwa sieci i informacji w obrębie Unii jako taki został przedstawiony w komunikacie Komisji Europejskiej w dniu 14 lutego 2013 roku. Niedługo zbliżymy się do trzech lat pracy nad dyrektywą, co jest raczej terminem dosyć długim. Standardowo tego typu projekty są prowadzone około dwóch lat, te bardziej skomplikowane – wyraźnie dłużej.

Proszę państwa, dyrektywa nie jest jakimś bardzo obszernym dokumentem, reguluje ona natomiast bardzo delikatną materię. W związku z tym jest duża dysproporcja pomiędzy różnymi krajami. Chodzi o sposób funkcjonowania, kwestie bezpieczeństwa, a nawet kwestie systemu w poszczególnych krajach. W związku z tym pomiędzy krajami członkowskimi były prowadzone bardzo poważne dyskusje w trakcie posiedzenia Grupy Roboczej H5 Rady Unii Europejskiej do Spraw Telekomunikacji i Społeczeństwa Informacyjnego, która działa przy Radzie do Spraw Transportu, Telekomunikacji i Energii. Jest kilka krajów, nawet nie tylko „starej” Unii Europejskiej, które posiadają już wewnętrzny system informowania się o pewnych incydentach. Dobierają one następne kraje do owego elitarnego klubu tylko i wyłącznie na zasadzie dobrowolności. Oczywiście, jest to nieformalna grupa. W związku z tym nie wszystkim krajom w oczywisty sposób tak jak Polsce i nowym członkom Unii Europejskiej zależało na pilnym przyjęciu projektu.

Polska od samego początku była bardzo dużym adwokatem dyrektywy. Byliśmy i cały czas jesteśmy mocno zaangażowani w prace nad jej kształtem. Na początku pracowały nad nią prezydencje: irlandzka, litewska, grecka, włoska, łotewska i luksemburska. Obecnie, proszę państwa, jesteśmy już na etapie zamknięcia szóstego nieformalnego *trilogu* z Parlamentem Europejskim. W dniu 7 grudnia odbył się ostatni *trilog*, podczas którego dyskutowano kwestie objęcia ograniczonym reżimem regulacyjnym dyrektywy tzw. *light touch* dostawców usług, czyli platform handlu elektronicznego, internetowych portali płatniczych, wyszukiwarek, usług chmurowych oraz sklepów z aplikacjami.

Proszę państwa, w dniu 18 grudnia 2015 roku odbyło się posiedzenie COREPER, podczas którego zaakceptowano przedstawiony przez prezydencję luksemburską proponowany tekst dyrektywy. Od tego czasu można uznać, że projekt dyrektywy jest już merytorycznie ustalony. Wiemy, czego ona dotyczy. Za chwilę będę o tym mówił troszkę bardziej szczegółowo. Wcale nie jest jednak powiedziane, że prace całkowicie się zakończyły. Jak wiadomo, diabeł tkwi w szczegółach. W związku z tym po trudnych pracach teraz dokument wymaga dopracowania pod kątem techniczno-legislacyjnym, pod kątem językowym, co wcale nie jest oczywiste. Zajmie to trochę czasu. Wydaje się nam, proszę państwa, że dyrektywa będzie przyjęta przez Parlament i Radę w pierwszej połowie 2016 roku. Pewnie będzie to bliżej połowy roku niż obecnego kwartału.

Co jest bardzo istotne, będzie dwadzieścia jeden miesięcy na implementację dyrektywy plus dodatkowe sześć miesięcy na kolejną kwestię, o której za chwileczkę będę mówił. Proszę państwa, pozornie wydaje się, że jest to krótki okres. Dwadzieścia siedem miesięcy jest to bardzo mało. Z tego powodu od pewnego czasu przygotowujemy się już do implementacji dyrektywy, nawet nie tyle implementacji dyrektywy, co do wprowadzenia w Polsce systemu, który, z jednej strony, w jakiś sposób będzie wprowadzał system ochrony cyberprzestrzeni w skali krajowej, a z drugiej strony, będzie na tyle przygotowany, żeby później odrębnym aktem prawnym nie trzeba było implementować dyrektywy. A więc chcemy na jednym ogniu upiec dwie pieczenie. Chcemy zbudować polski system na tyle nowoczesny, na tyle dopracowany, żeby nie było potrzeby odrębnej implementacji. Wydaje się nam to bardzo ważne z tego powodu, że jest konkretna presja czasowa, która będzie bardzo wyraźna. Od razu lepiej się pracuje, od razu wiadomo, że musimy skończyć do pewnego czasu. Dlatego przygotowujemy się do tego wcześniej.

Proszę państwa, w ministerstwie przy Komitecie Rady Ministrów do Spraw Cyfryzacji został powołany zespół zadaniowy, w skład którego wchodzą praktycznie wszyscy członkowie Rady Ministrów na poziomie co najmniej podsekretarzy stanu. Jest to nasze ciało polityczne, które decyduje o kierunkach prac nie tylko i wyłącznie nad dyrektywą, ale też nad systemem ochrony cyberprzestrzeni. Zespół spotyka się dosyć rzadko, ponieważ ma on podejmować zadania polityczne. Takie podejmuje, akceptuje też pewne prace merytoryczne prowadzone w ministerstwie razem z członkami grupy ekspertów. Przy zespole zadaniowym została powołana nieformalna grupa, w skład której wchodzą przedstawiciele Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa, Naukowej i Akademickiej Sieci Komputerowej, Ministerstwa Spraw Wewnętrznych i Administracji, policji, wojska. Pewnie kogoś pominąłem, ale generalnie są to te podmioty, które zajmują się bezpieczeństwem. Oczywiście, w razie potrzeby dopraszamy poszczególnych gości, żeby na poziomie eksperckim, nieformalnym mogli tylko i wyłącznie zająć stanowisko. Następnie grupa ekspercka przygotowuje swoje stanowisko, które jest akceptowane przez zespół zadaniowy, który następnie może to wszystko przedłożyć Komitetowi do Spraw Cyfryzacji. Formalna ścieżka pracy jest dosyć dobrze zorganizowana. Grupa ekspercka działa ponad rok. W zeszłym roku spotkała się ponad dwadzieścia razy. Prace są naprawdę systematyczne.

Jakie są braki w ochronie cyberprzestrzeni, mniej więcej wiadomo, ponieważ była bardzo poważna i gruntowna kontrola Najwyższej Izby Kontroli. Nie jest tajemnicą, że pomimo tego, iż w Polsce mamy zorganizowane na wysokim poziomie poszczególne jednostki, które faktycznie potrafią w znakomity sposób zabezpieczać, bronić nas przed atakami w cyberprzestrzeni, niestety, czasami ewidentnie brakuje zgrania systemowego wszystkich silosów – to po, żeby między sobą wymieniały informacje, żeby prace były w odpowiedni sposób, w efektywny sposób, koordynowane. Są to pewne braki, które, z jednej strony, nawet bez dyrektywy cały czas próbujemy rozwiązywać w Ministerstwie Cyfryzacji. W tym celu został też utworzony odpowiedni departament zajmujący się ochroną cyberprzestrzeni, który dopiero zaczyna działać. Jestem dyrektorem Departamentu Społeczeństwa Informacyjnego, powoli przekazuję swoje obowiązki nowym pracownikom. Ponieważ zajmowałem się tym trochę więcej i mam pewną pamięć historyczną, tylko z tego powodu właśnie ja to referuję.

Proszę państwa, krótko na temat samej dyrektywy. Generalną zasadą dyrektywy, jej celem jest wprowadzenie, osiągnięcie odporności na zagrożenia cybernetyczne w Unii Europejskiej. Jest to podstawowy cel, który wynika ze Strategii „Otwarta, bezpieczna i chroniona cyberprzestrzeń". Obecnie, proszę państwa, system mamy zagwarantowany tylko i wyłącznie na poziomie usług telekomunikacyjnych. Tymczasem wiadomo, że w obecnym czasie zdecydowanie mamy usługi dotyczące Internetu, usługi komunikacyjne, gdyż nie jest to tylko i wyłącznie telekomunikacja, ale są to usługi świadczone drogą elektroniczną, a więc szeroko rozumiany Internet. Poza tym, proszę państwa, jak powiedziałem, chcemy wprowadzić system scentralizowany na poziomie krajowym oraz podział kompetencji pomiędzy różne podmioty wymieniające informacje w oparciu o zbudowane mechanizmy współpracy.

Kolejną, proszę państwa, kwestią jest to, że dyrektywa zobowiązuje wszystkie państwa członkowskie do zagwarantowania minimalnego poziomu krajowych zdolności w dziedzinie bezpieczeństwa teleinformacyjnego poprzez, po pierwsze, ustanowienie właściwych organów do spraw bezpieczeństwa sieci i informacji, a następnie powołanie zespołów reagowania na incydenty komputerowe oraz przyjęcie krajowych strategii w zakresie bezpieczeństwa sieci i informacji. Oczywiście, nie jest tak, że nic, co dotyczy trzech punktów, które wymieniłem, w Polsce nie funkcjonuje, natomiast usystematyzowanie tego w pewien uporządkowany program, skoordynowany system jest absolutnie pożądane.

Poza tym, proszę państwa, dyrektywa NIS formułuje obowiązki służące zapewnieniu bezpieczeństwa sieci i informacji w sektorach rynkowych: energetyce, transporcie, bankowości i instytucjach finansowych, w sektorach zdrowia, zaopatrzenia w wodę i infrastruktury cyfrowej. Ponadto wprowadza mechanizmy współpracy państw członkowskich na dwóch poziomach. Po pierwsze, na poziomie technicznym. Mają to być osoby, które będą się zajmowały owymi kwestiami, osoby, które w cudzysłowie nazywamy osobami siedzącymi przy komputerze. Drugi poziom jest niemniej ważny, chociaż nie jest tak spektakularny, ponieważ nie pokazuje dużej serwerowni i osób siedzących przy komputerach. Jest to poziom polityczno-strategiczny, który wydaje się też bardzo istotny. Chodzi o to, żeby incydenty mogły być na pewno nie tyle załatwiane, ponieważ de facto politycy żadnego incydentu komputerowego jako takiego nie naprawią, tylko żeby mogły być wyciągnięte konsekwencje, przyszłe zabezpieczenia, wnioski wynikające z owych incydentów. Ma to być współpraca techniczna zapewniona poprzez europejską sieć CSIRT Computer Security Incydent Response Team oraz poprzez stworzenie mechanizmów wymiany informacji o incydentach transgranicznych pomiędzy CSIRT-ami narodowymi. Natomiast współpraca na poziomie polityczno-strategicznym ma być realizowana poprzez utworzenie grupy współpracy, która zajmuje się wypracowaniem wspólnym koncepcji. Proszę państwa, to tyle ogólnie na temat podstaw dyrektywy, tego, czemu ma ona służyć i w jaki sposób ma działać.

Jeżeli chodzi o kwestie troszeczkę bardziej szczegółowe, chciałbym powiedzieć, że zakres podmiotowy dyrektywy ujęty jest, proszę państwa, w Aneksie II do dyrektywy. Są tam wymienione podmioty z sektora prywatnego, jak i z sektora publicznego, dostarczające kluczowe usługi. Kluczowe usługi zostały zdefiniowane, obejmują one następujące sektory: energetyczny, transportowy, bankowy, finansowy, zdrowia, zaopatrzenia w wodę i infrastruktury cyfrowej.

Mówiłem, proszę państwa, że okres *vacatio legis* implementacji dyrektywy będzie wynosił dwadzieścia jeden miesięcy, ale na identyfikację sektorów jest jeszcze dodatkowe sześć miesięcy. Mamy więc dwadzieścia siedem miesięcy na implementację dyrektywy od czasu jej ogłoszenia, oczywiście w przetłumaczonej wersji, żeby było to zrozumiałe. Będzie to, proszę państwa, dużym wyzwaniem dla osób zajmujących się tą tematyką, ponieważ niełatwe będzie ustalenie progów, kiedy, np. sektor transportowy będzie się do tego zaliczał, a kiedy nie. Jest to duże wyzwanie. Ponadto, proszę państwa, operatorzy będą zobowiązani do dokonania oceny zagrożeń cybernetycznych, na jakie są narażeni, jak też do przyjęcia proporcjonalnych środków mających na celu zapewnienie bezpieczeństwa sieci i informacji. Podmioty te będą zobowiązane do zgłaszania właściwym organom wszelkich incydentów poważnie zagrażających sieciom i systemom informatycznym oraz mogących znacząco zakłócić ciągłość działania kluczowych usług.

Proszę państwa, właściwe organy do spraw bezpieczeństwa sieci i informacji będą miały uprawnienia do, po pierwsze, badania przypadków niewypełnienia przez operatorów zobowiązań z zakresu bezpieczeństwa sieci i informacji, następnie – oceny wyników audytów bezpieczeństwa teleinformatycznego, wydawania wytycznych w zakresie bezpieczeństwa teleinformatycznego oraz wprowadzania sankcji za nieprzestrzeganie przepisów. Będzie to też duże wyzwanie w przypadku ustawy, o której mówiłem – tego, jak będzie się ona nazywała, jeszcze nie ustaliliśmy, w cudzysłowie, ustawy o systemie ochrony cyberprzestrzeni – żeby wprowadzić wszystkie systemy, procedury. Podejrzewam, że samo wprowadzenie sankcji będzie powodowało bardzo dużo dyskusji, ponieważ w przypadku tego, co mi teraz przychodzi do głowy, a czym się zajmujemy, czyli

w przypadku ochrony danych osobowych sankcje są bardzo wysokie. Wynika to między innymi z tego, że wysokie sankcje gwarantują, iż można wprowadzić system, który jest troszeczkę mniej zbiurokratyzowany, ponieważ jesteśmy bardziej pewni, że odpowiednie podmioty będą bardziej zmobilizowane do tego, żeby przestrzegać wszystkich naszych wymagań.

Proszę państwa, jeżeli chodzi o dostawców usług cyfrowych, będzie obowiązywał tzw. *light touch approach* polegający na kontroli *ex post*, czyli po zaistnieniu incydentu, tylko przez państwo, na terenie którego dostawca usługi ma swoją siedzibę. Będzie to rozwiązanie podobne do tego, które jest w przypadku ochrony danych osobowych, które mamy w projekcie rozporządzenia o ochronie danych osobowych. Każdy podmiot będzie indywidualnie sprawdzany, będzie indywidualizowany na podstawie tego, gdzie znajduje się jego siedziba. Dostawcy usług cyfrowych są określeni w Aneksie III. Aneks III brzmi bardzo dumnie, ale obejmuje on tylko i wyłącznie trzy podmioty, czyli serwisy zakupowe, wyszukiwarki internetowe i usługi chmury obliczeniowej.

Dyrektywa nie dotyczy bezpośrednio usług administracji publicznej, o ile nie są to wymienione w dyrektywie usługi kluczowe. Podczas negocjacji w sprawie dyrektywy Polsce bardzo zależało na tym, żeby dyrektywa jednak była rozciągnięta na administrację publiczną, czego nie udało się wprowadzić. Kompromisem jest tylko to, że jest mowa o usługach kluczowych. Schodzimy się tylko w tym momencie. Nie ma natomiast żadnego problemu, żeby regulacja, którą wprowadzimy naszą, polską ustawą, obejmowała także administrację publiczną. Bardzo nam na tym zależy, żeby była ona jej elementem. Mówię zarówno o administracji rządowej, jak i o administracji samorządowej.

Na koniec, proszę państwa, powiem, że przepisy przewidują powołanie – co jest dla nas bardzo istotne, a co będzie elementem, trzonem, hubem systemu – jednego krajowego podmiotu do spraw bezpieczeństwa sieci i informacji na poziomie centralnym oraz dają możliwość poszerzenia kompetencji organów sektorowych. Oznacza to, że kraje członkowskie mogą wyznaczyć jeden CSIRT narodowy, a oprócz tego wprowadzić jeszcze CSIRT-y sektorowe, na których nam bardzo zależy. Zgodnie z naszym wstępnym podejściem do dyrektywy, wydaje się nam, że warto utrzymać CSIRT-y sektorowe, warto, żeby było ich jak najwięcej. Oprócz tego nad nimi powinien być jeden CSIRT narodowy, który będzie koordynował prace, który de facto będzie troszeczkę mniej techniczny, to znaczy, techniczny będzie musiał być, ale nie będzie pracował aż tak bardzo operacyjnie. Taka praca będzie wykonywana w CSIRT-ach sektorowych.

Na sali jest już pan minister. Jeżeli chodzi o ogólne pojęcie, myślę, że na początek może tyle wystarczy. Na sali jest też wiele osób, które zajmują się *stricte* tą tematyką. Wobec tego może już zakończę swoją wypowiedź.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję, panie dyrektorze. Chciałbym powitać pana ministra Witolda Kołodziejskiego, który również do nas dołączył. Nie wiem, czy pan minister chciałby coś dodać do tej wypowiedzi.

Sekretarz stanu w MC Witold Kołodziejski:

Szanowni państwo, pan dyrektor przedstawił bardzo szczegółową informację na temat wprowadzania nowej dyrektywy. Dodam tylko, że rzeczywiście jest to niesłychanie istotne. Cała tematyka „cyber" w tej chwili jest, można powiedzieć w cudzysłowie, tematyką modną. Po prostu docenia się powagę problemu. W zeszłym tygodniu miałem spotkania z delegacją ukraińską, delegacją ukraińskiego parlamentu. Jednym z głównych tematów, na które chciała ona rozmawiać, było cyberbezpieczeństwo, a wiedzą oni, co mówią, dlatego że z ich opisów wynikało, iż wojna na Ukrainie właściwie rozpoczęła się, trwa i pewnie będzie się kończyć głównie w cyberprzestrzeni. A więc tematyka cyberbezpieczeństwa jest dominującą tematyką, jeżeli chodzi o współczesne zagrożenia w obliczu konfliktu militarnego. Jest to tematyka bardzo istotna.

Jak wspomniał pan dyrektor, jest to prowadzone komplementarnie z innymi implementacjami prawa unijnego. Duże rozporządzenie o ochronie danych osobowych już wchodzi, też będzie implementowane. Tam sytuacja jest trochę inna, odwrotna, dlatego że będzie ono oddziaływało bezpośrednio, a więc musimy tylko tak zmienić prawo, żeby

umożliwić bezpośrednie oddziaływanie rozporządzenia o ochronie danych osobowych. Ochrona danych, bezpieczeństwo sieci są to te kierunki, w których dzisiaj podążają wszystkie dyskusje wokół rozwoju społeczeństwa informacyjnego, rozwoju technologii, rozwoju gospodarki. Musimy pamiętać, że wraz ze zwiększonym wzrostem uczestnictwa obywateli w świecie wirtualnym postępuje nie tylko wymiana informacji, ale przede wszystkim gospodarka oparta na nowoczesnych technologiach informacyjnych niesie również zagrożenia, na które musimy być przygotowani.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo uprzejmie dziękuję, panie ministrze. Chciałbym również poprosić o wypowiedzi instytucje, które są tutaj reprezentowane, a które uczestniczyły we wspomnianym przez pana dyrektora zespole zadaniowym. Może zaczniemy alfabetycznie. Agencja Bezpieczeństwa Wewnętrznego. Bardzo proszę o krótką wypowiedź. Uczestniczyliście państwo w całym tym procesie. Było około dwudziestu spotkań. Jak ustawa wygląda z państwa punktu widzenia?

Zastępca szefa Agencji Bezpieczeństwa Wewnętrznego płk Jacek Gawryszewski:

Bardzo dziękuję, panie przewodniczący. Jacek Gawryszewski, zastępca szefa Agencji Bezpieczeństwa Wewnętrznego.

Cały czas czekamy na ostateczny kształt dyrektywy, która będzie przyjęta, na to, jakie będą ostateczne regulacje. Oczywiście, mamy swoje doświadczenia w obszarze ochrony cyberprzestrzeni. Jest to temat, zjawisko bardzo złożone, interdyscyplinarne. Mamy świadomość możliwości różnych zagrożeń, zarówno tych, którymi Agencja zajmuje się na co dzień – chodzi o przeciwdziałanie terroryzmowi, szpiegostwo, proliferację, itd. – ale też wszystkich kwestii, które nie leżą w kompetencjach Agencji, a które też są zjawiskami występującymi na masową skalę i znacznie bardziej prozaicznymi w cyberprzestrzeni, takimi jak oszustwa, kradzieże, wymuszenia, fałszerstwa, itd. Jak mówię, tego rodzaju przestępczość nie leży w kompetencji Agencji, ale właśnie ten rodzaj przestępczej działalności póki co w cyberprzestrzeni znajduje najszersze odzwierciedlenie. Mamy doświadczenia, chociaż oczywiście dla nas też jest to stosunkowo nowe zjawisko. Mamy świadomość zagrożeń. Ostateczny kształt dyrektywy zdefiniuje naszą rolę w obszarze zabezpieczenia cyberprzestrzeni, identyfikowania zagrożeń, identyfikowania groźnych zjawisk. Zawsze pamiętamy o tym, że za każdą działalnością w cyberprzestrzeni, w świecie wirtualnym stoi człowiek. To też bierzemy pod uwagę próbując zdefiniować naszą rolę oraz kierunki naszych działań w zakresie bezpieczeństwa. Czekamy na ostateczny kształt dyrektywy. Zobaczymy, jaki będzie ostateczny wynik prac nad jej kształtem. Będziemy wówczas decydować, jaka będzie nasza rola w tym zakresie. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Mamy również przedstawicieli Komendy Głównej Policji. Czy chcieliby państwo zabrać głos? Bardzo proszę.

Pełnomocnik Komendanta Głównego Policji do spraw bezpieczeństwa cyberprzestrzeni kom. Marcin Kuskowski:

Panie przewodniczący, szanowni państwo!

Komisarz Marcin Kuskowski, pełnomocnik Komendanta Głównego Policji do spraw bezpieczeństwa cyberprzestrzeni.

Chciałbym powiedzieć, że w policji są podejmowane działania związane z przygotowaniem naszej infrastruktury oraz zespołu POL-CERT do reagowania na incydenty komputerowe, zespołu który został powołany przez Komendanta Głównego Policji, zespołu do współpracy i działań w zakresie związanym z procesem reagowania na incydenty w istniejącej infrastrukturze internetowej. Oddzielona została rola związana z ochroną infrastruktury policji od działań związanych ze zwalczaniem cyberprzestępczości. Jest zbudowany cały system, są powołane, ustanowione wydziały do walki z cyberprzestępczością. Na poziomie Komendy Głównej Policji jest wydział, który koordynuje prace wydziałów terenowych. W tym momencie skupiamy się na kwestii związanej z procesem reagowania w przypadku wykrycia incydentów oraz na ścisłej współpracy z Agencją

Bezpieczeństwa Wewnętrznego i Rządowym Zespołem Reagowania na Incydenty Komputerowe. Dziękuję.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo uprzejmie dziękuję. Otwieram dyskusję. Zapraszam posłów do zadawania pytań. Bardzo proszę. Pierwszy do zadania pytania zgłosił się pan poseł Maciej Małecki.

Poseł Maciej Małecki (PiS):

Dziękuję bardzo. Mam jedno pytanie. Projekt dyrektywy przewiduje rozwiązywanie problemu zabezpieczenia poprzez tworzenie jednego CSIRT-u ogólnokrajowego bądź kilku sektorowych. Jaką koncepcję uważacie państwo za lepszą dla Polski? Jaką będziecie proponowali?

Sekretarz stanu w MC Witold Kołodziejski:

Projekt nie wyklucza i jednego, i drugiego rozwiązania, umożliwia tworzenie i CSIRT-u narodowego, i CSIRT-ów sektorowych. Opowiadamy się za połączeniem obydwu koncepcji, czyli stworzeniem CSIRT-u narodowego plus określonych CSIRT-ów sektorowych. Oczywiście, granice CSIRT-ów sektorowych będą przedmiotem kolejnych dyskusji. Zapomniałem dodać, że przy implementacji dyrektywy będziemy prowadzili bardzo głębokie, bardzo szerokie konsultacje. Ponieważ dotyczy ona tak różnych sfer rynku oraz w ogóle funkcjonowania społecznego, konsultacje niewątpliwie będą musiały być bardzo szerokie. Na dzisiaj najrozsądniejsze rozwiązanie, jakie przychodzi nam do głowy – mówię to w kontekście konsultacji, które jeszcze będziemy prowadzili, ponieważ były tutaj różne zdania – to jeden ośrodek narodowy i przynajmniej kilka sektorowych w sektorach, które zidentyfikujemy jako najbardziej narażone na zagrożenia.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Kto z pań i panów posłów chciałby zadać kolejne pytanie? Jeżeli nie ma, może ktoś z gości, których mamy. Jeżeli nie ma, mam kilka pytań. Czy państwo w swoich pracach napotkaliście na jakieś ryzyka, które dla naszego kraju będą się wiązały z wprowadzeniem ustawy? Z jednej strony, jest to współpraca w ramach Unii Europejskiej, ale też, jak się domyślam, otwarcie naszych systemów obrony albo też współpraca owych systemów z systemami innych krajów. Jak to jest rozwiązane na gruncie ustawy, na gruncie planów?

Dyrektor departamentu w MC Maciej Groń:

Oczywiście, największe wyzwanie, które, jak mi się wydaje, istnieje w przypadku prac, polega na tym, żeby projekty procedury, które przygotujemy, procedury reagowania na poszczególne incydenty, były w praktyce realne do zastosowania. Z reguły jest tak, że w szczególności w działce ochrony cyberprzestrzeni bardzo często wymiana informacji jest nieformalna, po prostu chwyta się za telefon, czasu jest bardzo mało. Wydaje mi się, że w związku z tym bardzo skomplikowane dla nas będzie to – mam nadzieję, że później państwo posłowie nam pomogą – żeby wdrożyć przepisy, które będą mało zbiurokratyzowane, ponieważ będzie nam zależało na szybkiej wymianie informacji, na możliwości szybkiego działania poszczególnych służb. Wiem, że CSIRT japoński działa tak, że jest jeden główny narodowy, a oprócz tego jest sześćdziesiąt CSIRT-ów sektorowych. Wszystkie mają porozumienie dotyczące wymiany informacji przypieczętowane uściskiem dłoni. Nasze tradycyjne podejście do przepisów, do procedur może spowodować, że automatycznie wprowadzimy jakieś zasady, które później uniemożliwią to, żeby system był wydolny. Tak naprawdę, właśnie to wydaje mi się dużym problemem i zagrożeniem dla nas. Oczywiście, jeszcze tego nie ma, jeszcze tego nie napisaliśmy, ale trzeba sobie wyraźnie powiedzieć, że nie może być tak, iż z ustawy będzie dokładnie wszystko wynikało, że na wszystko będzie procedura, ponieważ technologie się zmieniają. Będą to musiały być rozwiązania, które wiadomo, że nie będą odporne na czas. Wiadomo, że ustawę co jakiś czas trzeba będzie nowelizować, ale chodzi o to, żeby nie trzeba było tego robić raz na rok, ale, np. raz na pięć lat. Jestem prawnikiem, więc z mojego punktu widzenia właśnie to wydaje mi się najtrudniejsze. Dla osób, które są osobami „technicznymi", pewnie jest jeszcze wiele innych zagrożeń.

Przewodniczący poseł Paweł Pudłowski (N):

Nie całkiem o to pytałem. Pytałem o ryzyka międzynarodowe. Rozumiem, że ich nie dostrzegacie. Czy tak? Rozumiem. Kolejne pytanie dotyczy pracy silosowej, o której sam pan dyrektor wspomniał. Pojawia się to też w jednym z raportów Najwyższej Izby Kontroli, że kwestia cyberprzestępczości, cyberbezpieczeństwa często jest rozwiązywana w sposób silosowy w departamentach, w ministerstwach. Moim zdaniem, państwo bardzo fajnie wyszliście z inicjatywą powołania zespołu ekspertów, który skupia wiele obszarów, wiele instytucji krajowych. W jaki sposób zagwarantujecie, że praca ta dalej będzie właśnie w taki sposób toczona? Jak wewnątrz poszczególnych instytucji wygląda przekazywanie informacji o procedowaniu nad ustawą, przygotowywanie się do ustawy?

Sekretarz stanu w MC Witold Kołodziejski:

Są dwie rzeczy, jedna, jeżeli chodzi o procedowanie nad ustawą implementującą dyrektywę, druga, jeżeli chodzi o funkcjonowanie całego systemu. Jeżeli chodzi o funkcjonowanie całego systemu, jest to to, o czym mówił pan dyrektor Groń. Jest to przejście, komunikacja pomiędzy silosami, z tym że, co istotne, silosy te dzisiaj nie są tak definiowane jak silosy resortowe. Mówimy o podobnie zdefiniowanym poziomie zagrożenia wypływającego z podobnych przyczyn. Strefy transportowa, telekomunikacyjna lub inna często są to rzeczy łączące tak naprawdę wiele różnych resortów. Po pierwsze, praca nad implementacją nie może być silosowa. Jak mówiłem, szerokie konsultacje to nie tylko szerokie konsultacje międzyresortowe, które są niezbędne po to, żeby chociażby wyznaczyć obszary CERT-ów bądź CSIRT-ów sektorowych, ponieważ będą one przekraczały granice resortowe. Z drugiej strony, praca nad implementacją musi przekraczać sferę resortową, ponieważ musi ona iść znacznie szerzej w sferę przedsiębiorczości, biznesu, itd. Na przykład, jeżeli chodzi o sektor bankowy, ze względu na wielość zagadnień, których on dotyczy – są tutaj transakcje internetowe, ale też narzędzia autoryzacyjne, wymiana informacji, o czym wspominał pan przewodniczący – sięgamy już poziomu międzynarodowego w skali Europy, ale też poziomu międzykontynentalnego, ponieważ tam sięga wymiana informacji, zresztą także w wielu innych obszarach. A więc tradycyjne pojęcie silosów resortowych z miejsca musi być rozbite, dlatego że inaczej sobie z tym nie poradzimy. Na poziomie samej implementacji chcemy zrobić szerokie konsultacje, oczywiście, najpierw także międzyresortowe, ponieważ będzie to propozycja rządowa, ale później wychodzące daleko poza resorty, przede wszystkim konsultacje ze sferą biznesową. Rozwiązania dotyczące cyberbezpieczeństwa w niektórych gałęziach są bardzo zaawansowane, jak chociażby w sektorze bankowym lub telekomunikacyjnym. Są tam wypróbowywane najnowsze technologie w dziedzinie cyberbezpieczeństwa. A więc będziemy się też od nich uczyli, będziemy czekali na propozycje od nich. Jedna rzecz to praca w ramach szerokich konsultacji.

Po drugie, jeżeli chodzi o sektory, które będą wyznaczone, jak mówił o tym pan dyrektor, rzeczywiście, jest zagrożenie braku sprawnej komunikacji. Nie boimy się, że nie będzie żadnej komunikacji, tylko że akurat w tej dziedzinie komunikacja jest tak błyskawiczna, że reakcja musi być równie błyskawiczna, musi nadążyć. A więc nie ma tutaj możliwości pozostawiania jakichś mechanizmów, przeszłych technologii, np. dzwonienia na telefon na biurko. Nie ma o tym mowy. Musimy opracować sprawną technologię komunikacji, ale też technikę oraz rozwiązania ustrojowe, które będą, mówiąc w cudzysłowie, odporne na postęp technologiczny. Chodzi o to, żeby nie było tak, że nasze prawo po pół roku przez przestępców, cyberterrorystów zostanie wyprzedzone na tyle, że nasze rozwiązania będą stanowiły poważne zagrożenie ze względu na zacofanie, nieprzewidzenie różnych konsekwencji technologicznych. Dzisiejsza silosowość, zagrożenie silosowością przenosi się na zamknięcie konkretnych, szczegółowych CSIRT-ów. System bezpieczeństwa musi być na tyle odporny, na tyle uniwersalny, żeby działał w każdej, nawet trudnej do przewidzenia sytuacji. Dziękuję bardzo.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję za wyczerpującą odpowiedź. Proszę.

Dyrektor departamentu w MC Maciej Groń:

Chciałbym dopowiedzieć, w jaki sposób nasze ministerstwo jest otwarte na współprace, na wymianę informacji po to, żeby być lepiej poinformowanym. Na podstawie „Polityki Ochrony Cyberprzestrzeni RP" powołaliśmy około stu pięćdziesięciu pełnomocników do spraw ochrony cyberprzestrzeni. Praktycznie każdy resort posiada swojego pełnomocnika. Stanowi on punkt kontaktowy, żeby wymieniać między sobą informacje, żeby było wiadomo, że jest konkretny człowiek pod konkretnym *e-mailem*. *E-mail* tworzymy w ten sposób, że po wyrazie „pełnomocnik" mówimy o resorcie, a nie podajemy nazwisko, ponieważ jest bardzo prawdopodobne, że osoby te co jakiś czas mogą się zmieniać. Są one z administracji rządowej, ale jest też bardzo wiele osób z administracji samorządowej. Średnio raz na dwa, trzy miesiące organizujemy dla pełnomocników szkolenia, z jednej strony, po to, żeby podnosili oni swoje kompetencje, z drugiej strony, po to, żeby spotykali się nie tylko w świecie wirtualnym, ale też w świecie realnym, żeby poznali się w trakcie wspólnej kawy bądź w czasie dojazdów na szkolenia do Warszawy albo gdzie indziej. Mam nadzieję, że dzięki temu od razu będzie się im lepiej współpracowało. W różnych przerwach pomiędzy wykładami będą wymieniali swoje doświadczenia. Angażujemy ich, próbujemy stworzyć społeczeństwo, które będzie się specjalizowało w tej tematyce. Wydaje mi się, że dodatkowo jest to duża wartość dodana.

Przewodniczący poseł Paweł Pudłowski (N):

Bardzo dziękuję. Mam pytanie o koszty. Czy jesteście już państwo na etapie szacowania kosztów stworzenia scentralizowanego systemu? Jest jeszcze za wcześnie, tak? Dobrze.

Czy macie państwo jeszcze jakieś pytania? Pan przewodniczący? Nie.

Sekretarz stanu w MC Witold Kołodziejski:

Panie przewodniczący, ponieważ okres implementacji dyrektywy dopiero się zacznie, w tej chwili nie mamy policzonych kosztów, nie jesteśmy w stanie tego policzyć, ale jedno już wiemy, że na pewno będą. Jest to nieuniknione, niestety.

Przewodniczący poseł Paweł Pudłowski (N):

Szanowni państwo, wobec tego zamykam dyskusję. Stwierdzam, że porządek dzienny został wyczerpany.

Protokół z posiedzenia z załączonym zapisem jego przebiegu będzie do wglądu w sekretariacie Komisji w Kancelarii Sejmu. Bardzo uprzejmie dziękuję. Do widzenia.